



Ingate Firewall

interworking with

SSH Sentinel

Tested versions:
Ingate Firewall 3.2.0
SSH Sentinel 1.4 (build 177, 190) and 1.4.1 (build 79) on Windows XP

1. Install the SSH Sentinel software on the client machine according to the instructions

Note: Depending on certificate management you will have to choose the proper certificate signing method. Accepted are X.509 certificates signed by a local CA server, a CA server on the Internet or a self-signed certificate. A pre-shared key is not supported for road warriors on the Ingate Firewall.

2. Certificate configuration on your Ingate Firewall

a) If you are going to use self-signed certificates follow these steps:

Create the certificate on the **Local X.509 Certificate** page by pressing the Create a self-signed X.509 certificate button.

Send the file so that the Sentinel client can access it.

Import the self-signed certificate from the Sentinel Client. For more information about that see section 6.

b) Or if you are going to use a CA-server to sign the certificates:

Import the CA's own certificate under **Virtual Private Networks – Trusted VPN CA**

Create a certificate requests on the **Local X.509 Certificate** page by pressing the Create an X.509 certificate request button.

Download the file so that the CA server can access it and sign the certificate request.

When the certificate request is signed by the CA, import the certificate on the **Local X.509 Certificate** page.

3. VPN configuration on your Ingate Firewall

To configure the VPN tunnel go to the **IPsec Peers** page:

Add a new row.

Select a suitable name for the client and make the following settings:

Authentication type = Trusted CA (even when using self-signed certificates).

On Authentication info select the name used when the certificate was imported.

Local side = Normally the external interface, otherwise the interface closest to the client.

Remote side = *

On/Off = Active

On the **Tunneled Networks** page:

Add a new row and make the following settings:

Peer = Select the one configured on the **IPsec Peers** page.

Local side of network = Select the network address and netmask for your local network that should be accessible through the VPN tunnel.

Remote side of network = Select * in the address field and leave the netmask field empty.

4. Certificate configuration on the SSH Sentinel

Now start the SSH Sentinel Policy Editor and click on the Key Management tab.

a) If you are using self-signed certificates follow these steps:

Import the self-signed certificate from the Ingate Firewall.

Go to the Key Management tab and select Add under Trusted Certificates – Remote Hosts.

Select the file you downloaded from the firewall and verify that it is the correct certificate, and accept when prompted to do so.

b) Or if you are going to use CA signed certificates

Import the CA's own certificate. Under Trusted Certificates – Certification Authorities select Add and choose the CA certificate file.

To create a certificate request for the CA to sign, go to My Keys – host keys – Add. When the dialogue (see figure 1) New authentication key appears choose to Enroll for a certificate.

If you want to create a new key pair for the certificate request instead choose Create an authentication key pair and a certificate. This will create a new key pair instead of using the ones created during installation.

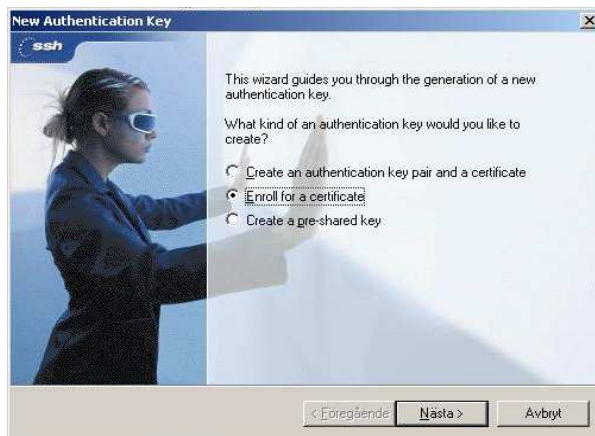


Figure 1. To create a certificate request

In the next dialogue click next. If you wish to add some information (or change the Common name) press the Advanced button.

Under Certificate Enrollment (see figure 2) choose to Create a certification request and save it in a file for later enrollment. Send or save the *.req file so that the CA server can access it.



Figure 2. Certificate enrollment

When the certificate is signed and delivered back the certificate must be imported. This is done under the Key Management tab. Select My Keys and right-click on host key (under where the certificate request is) and then import the certificate.

5. VPN configuration on the SSH Sentinel

Start the Policy Editor and click on the Security Policy tab.

Click on VPN Connections and Add

Gateway name needs the IP address (or name) of the Ingate Firewall.

Remote network defines the network behind the firewall that the client is allowed to access. If the network is not already predefined use the button to the right and add a new network.

Select the certificate you want to use for this connection.

Press OK.

6. Exporting the self-signed Sentinel certificate

To export the self-signed Sentinel client certificate.

Select your certificate in the SSH Sentinel client.

Under My Keys on the Key Management page, click View and then Export to save the key as a file.

On the firewall go to the **Trusted VPN CA** page and add a new CA. Select the file exported from the client and give it a suitable name.

7. The final configuration touch

Check that the remote network in the Sentinel client matches the one configured in the Ingate Firewall on the **Tunneled Networks** page.

Also make sure that the correct certificates are imported. If you are using self-signed certificates do not use X.509 certificates as Authentication type on the **IPsec Peers** page of the Ingate Firewall. The correct choice is Trusted CA.

If the Sentinel client is using NAT you will have to configure the Ingate Firewall a bit more.

The Remote side on the **Tunneled Networks** page needs to have the client's local IP address (i.e. with no NAT applied), and Allow subset set to Yes.

For setup and testing purposes it can be useful to deactivate blacklisting. This is done on the **IPsec Status and Settings** page under Blacklisting. Set the interval to 0 (zero). Remember to change that value when you are done with the tests.

Now, if everything seems to be configured, try the Diagnostics function on the Sentinel Client. Go to the Security Policy tab – VPN Connections, select your connection and press Diagnostics. If everything is fine you should get a message that says it is possible to establish an IPsec protected connection, see figure 3.

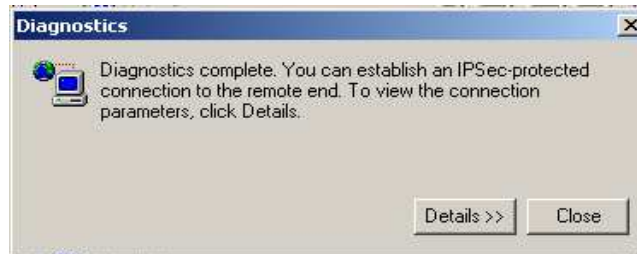


Figure 3 Successful diagnostics test

8. Using SIP on Ingate Firewalls with Sentinel Client

When the Ingate Firewall will be used with SIP and a user with a Sentinel client wants to register on the Ingate Firewall, some additional configuration has to be done on the firewall as well as the Sentinel client.

On the Sentinel, repeat the steps in section 5. Use the same Gateway name/IP address but the remote network should now be same as the Gateway name/IP address (netmask 255.255.255.255).

On the Ingate Firewall, add the same information on the **Tunneled Networks** page. This configuration makes it possible to register on the SIP server.

The Sentinel normally only allows one concurrent VPN tunnel and that is fine as long as you only need to access remote resources or use SIP. If both is required we need to have at least two concurrent VPN tunnels up.

This is configured by highlighting the connection under Security Policy – VPN Connections, then press Properties. In the display that shows select the Advanced tab and there check the Open on start-up box (see figure 4).

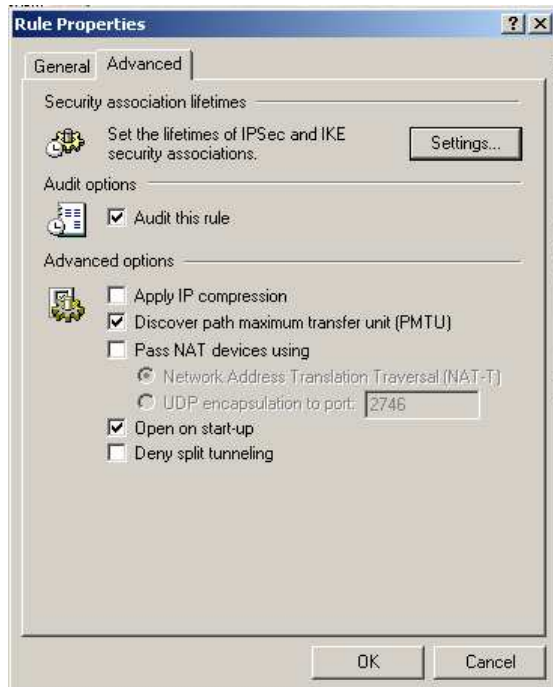


Figure 4. Configure more than one concurrent VPN tunnel

Repeat this for the other concurrent VPN tunnel needed. The next step, section 9, is not required when checking that box.

9. Connecting to the Ingate Firewall

In the task bar the Sentinel Agent Icon should be visible. Right-click on the icon, go to Select VPN and select the VPN connection you want to use.



Figure 5. Taskbar icon



Figure 6. Taskbar menu

10. More advanced functionality in the SSH Sentinel

For more configuration possibilities read the SSH User Manual.